



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/556,945	04/21/2000	James D. Marks	3042/OG956	6556

7590 10/07/2003  
Darby & Darby PC  
805 Third Avenue  
New York, NY 10022

EXAMINER

MORGAN, ROBERT W

ART UNIT PAPER NUMBER

3626

DATE MAILED: 10/07/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No. 09/556,945	Applicant(s) MARKS, JAMES D.
Examiner Robert W. Morgan	Art Unit 3626

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 20 July 2003.
- 2a)  This action is **FINAL**.
- 2b)  This action is non-final.
- 3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4)  Claim(s) 1-148 is/are pending in the application.  
4a) Of the above claim(s) 73-148 is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-72 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) 73-148 are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  The drawing(s) filed on \_\_\_\_\_ is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11)  The proposed drawing correction filed on \_\_\_\_\_ is: a)  approved b)  disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12)  The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_ .  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 14)  Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
a)  The translation of the foreign language provisional application has been received.
- 15)  Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_ .
- 4)  Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_ .
- 5)  Notice of Informal Patent Application (PTO-152)
- 6)  Other: \_\_\_\_\_ .

Art Unit: 3626

## **DETAILED ACTION**

### ***Response to Amendment***

1. In the amendment filed 7/20/03 in paper number 7, the following has occurred: Claims 1, 3, 4, 15, 25, 27, 28, 31-34, 45, 46, 51 and 53 have been amended and claims 63-148 have been added. Now claims 1-148 are presented for examination.

### ***Election/Restrictions***

2. Newly submitted claims 73-148 are directed to an invention that is independent or distinct from the invention originally claimed for the following reasons: on-line consent to volunteering for consideration as potential candidate for one of a potential clinical trial and a clinical trial in progress.

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 73-148 withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

### ***Claim Objections***

3. The claim objection to claim 31 has been withdrawn by the Examiner based on the changes made by Applicant to the claim.

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 3626

5. Claims 1-20, 25-50 and 52-72 and are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,731 to Colon et al. in view of U.S. Patent No. 6,171,112 to Clark et al.

As per claim 1, Colon et al. teaches an Internet-networked system with online communication to a computing center from a large number of clinical study investigators at numerous and diverse locations remote from the computing center (see: column 1, lines 36-38). In additions, the system handles automatic assignment and randomization of thousands of participants in a clinical study with respect to care strategies to be administered to the study participants (see: column 1, lines 48-51). Furthermore, the system captures data in its database through appropriate input forms developed for the specific clinical study and the data is stored online and reports are produced in real time to study investigators (reads on “release of at least one of medical and personal information”) and to the sponsor regarding sites that are participating, recruitment levels by participating site, patient follow-up, and significant events (see: column 1, lines 64 to column 2, lines 4).

Colon et al. fails to teach the claimed on-line consent to an electronic agreement relating to the release of at least one of medical and personally identifying information.

Clark et al. teaches a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50). The Examiner considers using a name as the electronic signature, which is unique to each person as a personally identifying information.

Art Unit: 3626

One of ordinary skill in the art at the time the invention was made would have found it obvious to include authenticating informed consent for patient as taught by Clark et al. within the method for managing data used in conducting clinical studies as taught by Colon et al. with the motivation of positively affecting the patient-physician relationship by allowing the physician to accomplish more with each patient in less time (see: Clark et al.: column 3, lines 37-40).

As per claim 2; Clark et al. teaches the electronic agreement is a click wrap consent agreement (see: Fig. 17).

As per claim 3, Clark et al. teaches the claimed generating an electronic survey form to be displayed at the computer terminal. This limitation is met by the computer system (17, 18, 19, Fig. 1) with a screen that brings up a form used for entering patient related data (see: column 6, lines 22-30).

As per claim 4, Colon et al. teaches the claimed electronic survey form comprises at least one of personally identifying and medical related questions. This feature is met by the computer system (17, 18, 19, Fig. 1) with a screen that brings up a form used for entering patient related data such as identification, demographics and medical conditions and later transmitted to the study management center (10, Fig. 1) as represented by input block (61, Fig. 5) (see: column 6, lines 22-30).

As per claims 5-7, Colon et al and Clark et al. teaches a method of obtaining an informed patient consent during a patient session, which includes the answering of questions by the patient and this data is encrypted and transmitted to a central data facility (see: column 4, lines 31-55). In addition, the data maybe transferred via the Internet, a dedicated local area network, leased private or semi-private data transmission lines using encryption or other secure means (see:

Art Unit: 3626

Clark et al.: column 10, lines 54-57). Furthermore, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claims 8-15, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44). Colon et al. and Clark et al. also teach a method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). Colon et al. and Clark et al. further teach that transferred data from the data facility (702, Fig. 7) to the Virtual Interactive Teaching and Learning (VITAL) Centers is updated to ensure that the information is up-to-date and accurate (see: Clark et al.: column 17, lines 26-30 and Fig. 9). Colon et al. and Clark et al. also teach that only authorized personnel can access the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of patient information (see: Clark et al.: column 12, lines 58-61). The Examiner considers the authorized personnel accessing the system as the only users providing requests and responses to retrieve data from the memory devices.

As per claim 16, Colon et al. and Clark et al. teach the claimed generating a certificate to verify transmission between the individual and the secure server. This limitation is met by the patient being asked sign an informed consent electronically and acknowledge of the consent is printed (see: Clark et al.: column 4, lines 19-22). In addition, Colon et al. and Clark et al. teach

Art Unit: 3626

the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claim 17, Colon et al. teaches a computer terminal employing a web browser capable of supporting a secure socket layer protocol (see: column 39-41).

As per claim 18, Colon et al. and Clark et al. teach the claimed ensuring decrypted data stored at said secure server is not accessed by unauthorized personnel. This feature is met by the method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). Clark et al. also teaches that only authorized personnel can access the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of patient information (see: Clark et al.: column 12, lines 58-61). In addition, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claim 19, Colon et al. and Clark et al. teaches the claimed ensuring step comprises at least one of limiting access to said secure server to a minimum number of authorized personnel, identifying as authorized personnel only trustworthy employees, and devising and implementing procedures to ensure that only authorized personnel gain access to the decrypted data. This feature is met by allowing only authorized personnel to access the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of

Art Unit: 3626

patient information (see: Clark et al.: column 12, lines 58-61). In addition, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claim 20, Colon et al. and Clark et al. teach the claimed generating using said secure server an electronic opt-out form to be displayed on the computer terminal to remove the individual's name from a list of consenting individuals. This limitation is met by the eligibility routine, where an determination is made at the time when patient data is submitted, whether the patient qualifies for the clinical study, and if not, a message is communicated to the clinical study investigator's computer (see: Colon et al.: column 2, lines 5-9). In addition, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44). The Examiner considers the message sent to the study investigator's computer regarding eligibility as a form of removing an individual from participating or consenting to the clinical study.

As per claim 25, Colon et al. teaches an Internet-networked system with online communication to a computing center from a large number of clinical study investigators at numerous and diverse locations remote from the computing center (see: column 1, lines 36-38). In additions, the system handles automatic assignment and randomization of thousands of participants in a clinical study with respect to care strategies to be administered to the study participants (see: column 1, lines 48-51). Furthermore, the system captures data in its database through appropriate input forms developed for the specific clinical study and the data is stored online and reports are produced in real time to study investigators and to the sponsor regarding



Art Unit: 3626

sites that are participating, recruitment levels by participating site, patient follow-up, and significant events (see: column 1, lines 64 to column 2, lines 4).

Colon et al. fails to teach the claimed on-line consent to an electronic agreement relating to the release of at least one of medical and personally identifying information.

Clark et al. teaches a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50). The Examiner considers using a name as the electronic signature, which is unique to each person as a personally identifying information..

The obviousness of combining the teachings of Colon et al. and Clark et al. are discussed in the rejection of claim 1, and incorporated herein.

As per claims 26-30, they are rejected for the same reasons set forth in claims 2-4 and 6-7 respectively.

As per claim 31, Colon et al. teaches an Internet-networked system with online communication to a computing center from a large number of clinical study investigators at numerous and diverse locations remote from the computing center (see: column 1, lines 36-38). In additions, the system handles automatic assignment and randomization of thousands of participants in a clinical study with respect to care strategies to be administered to the study participants (see: column 1, lines 48-51). Furthermore, the system captures data in its database through appropriate input forms developed for the specific clinical study and the data is stored online and reports are produced in real time to study investigators (reads on “release of at least one of medical and personal information”) and to the sponsor regarding sites that are

Art Unit: 3626

participating, recruitment levels by participating site, patient follow-up, and significant events (see: column 1, lines 64 to column 2, lines 4). In addition, Colon et al. teaches the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: column 3, lines 24-44).

Colon et al. fails to teach the claimed on-line consent to an electronic agreement relating to the release of at least one of medical and personal information.

Clark et al. teaches a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50).

The obviousness of combining the teachings of Colon et al. and Clark et al. are discussed in the rejection of claim 1, and incorporated herein.

As per claims 32-33, they are rejected for the same reasons set forth in claims 3-4.

As per claim 34, Colon et al. teaches wherein at least one computer terminal is used to enter at least one of personally identifying and medical data in response to the questions in the electronic survey form. This feature is met by the computer system (17, 18, 19, Fig. 1) with a screen that brings up a form used for entering patient related data such as identification, demographics and medical conditions and later transmitted to the study management center (10, Fig. 1) as represented by input block (61, Fig. 5) (see: column 6, lines 22-30).

As per claims 35-42, they are rejected for the same reasons set forth in claims 17, 6 and 8-13, respectively.

Art Unit: 3626

As per claim 43, Colon et al. teaches the claimed secure server and central office are a single device at the same location. This limitation is met by the study management center (10, Fig. 1) at a particular geographical site that includes a database host computer (11, Fig. 1) connected via network (12, Fig. 1) to an Internet server (13, Fig. 1) (see: column 2, lines 58-64).

As per claims 44-46, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44). Colon et al. and Clark et al. also teach a method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). Colon et al. and Clark et al. further teach a system that includes a study management center (10, Fig. 1) at a particular geographical site that includes a database host computer (11, Fig. 1) connected via network (12, Fig. 1) to an Internet server (13, Fig. 1) (see: Colon et al.: column 2, lines 58-64). In addition, the Internet server (13, Fig. 1) uses Netscape Secure Server software to provide encryption of all material moving to and from the central Internet server (see: Colon et al.: column 3, lines 35-38). Moreover, Colon et al. and Clark et al. also teach that only authorized personnel can access the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of patient information (see: Clark et al.: column 12, lines 58-61). The Examiner considers the authorized personnel accessing the system as the only users providing requests and responses to retrieve data from the memory devices.

Art Unit: 3626

As per claims 47-50 and 52-54, they are rejected for the same reasons set forth in claims 17-20, 7, 20 and 19, respectively.

As per claim 55-56, Colon et al. and Clark et al. teach the on-line recruitment is of candidates for clinical trials and the individual is an end user. This limitation is met by the eligibility routine, where a determination is made regarding the patient submitted data as to whether the patient is qualified for the clinical study. The eligible patients are identified immediately on-line while they are still in the physician's office (see: Colon et al.: column 1, lines 64 to column 2, lines 12). Colon et al. and Clark et al. further teach a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: Clark et al.: column 11, lines 66 to column 12, lines 50).

As per claim 57 and 62, they are rejected for the same reasons set forth in claim 20.

As per claim 58-61, they are rejected for the same reasons set forth in claims 55-56.

As per claim 63, Clark et al. teaches the claimed displaying the electronic survey form in response to receipt of the individual's consent to the electronic agreement. This limitation is met by an individual seeking informed consent and selecting the appropriate survey that requires authentication of the recipient's (see: column 6, lines 33-36).

As per claim 64, Colon and Clark et al. teach the claimed authorized individual reviews the encrypted processed data and selected a potential candidate volunteer as a potential candidate is met by the only authorized personnel accessing the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of patient information (see: Clark et al.: column 12, lines 58-61), the method comprising:

Art Unit: 3626

--the claimed communicating to the potential candidate volunteer the selection as the potential candidate is met by the user table (48, Fig. 4) that contains contact information related to the user (see: Colon et al.: column 5, lines 17-20).

As per claim 65, Colon teaches the claimed communication comprises one of:

(a) the central office contacting the potential candidate in order to request permission for the authorized individual to contact the potential candidate;

(b) the central office providing the authorized individual with contact information for the potential candidate and the authorized individual communicating with the potential candidate;  
and

(c) the central office communicating to the potential candidate the selection and providing contact information for the potential candidate to initiate contact with the one of the authorized individual and an employee of the clinical trial associated with the authorized individual.

Colon et al. teach the claimed (b) the central office providing the authorized individual with contact information for the potential candidate and the authorized individual communicating with the potential candidate. This limitation is met by the user table (48, Fig. 4) that contains contact information related to the user (see: column 5, lines 17-20). In addition, Colon et al. teaches a permission table (49, Fig. 4) that contains flags that are used to authorize a user for access to information about sites, regions and study level information (see: column 5, lines 17-25).

As per claim 66, Clark et al. teaches the claimed personally identifying information is one or name, address, telephone number, e-mail address and name with birth date. This limitation is

Art Unit: 3626

met by the method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50). The Examiner considers using a name for the electronic signature, which is unique to each person, as example of personally identifying information.

As per claims 67-68, they are rejected for the same reason set forth in claims 63 and 66.

As per claims 69-70, they are rejected for the same reason set forth in claims 32 and 46.

As per claims 71-72, they are rejected for the same reason set forth in claims 65 and 66.

6. Claims 21, 24 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,731 to Colon et al. and U.S. Patent No. 6,171,112 to Clark et al. in view of Official Notice.

As per claim 21, Colon et al. and Clark et al. fail to teach the claimed electronic agreement satisfies all federal, state, and local rules, ordinances and regulations.

However, it is well known in the computer field that electronic agreements or contracts use and follow all federal, state, and local rules, ordinances and regulations with regard to the dissemination of medical, health and personally identifying information. Therefore, it would have been obvious a person of ordinary skill in the art at the time the invention was made to include an electronic agreement that satisfies all federal, state, and local rules, ordinances and regulations with regard to the dissemination of medical, health and personally identifying information with the combined system of Colon et al. and Clark et al. with the motivation of avoiding the any negligent and malpractice litigation caused by not stating and following all federal, state, and local rules, ordinances and regulations.

Art Unit: 3626

As per claim 24, Colon et al. and Clark et al. fail to explicitly teach encryption keys stored on a disk kept under physical surveillance.

However, Colon et al. and Clark et al. teach method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). It is well known in the computer industry for a person to be possession of a disk used to store standard private/public encryption and decryption keys as described by Colon et al. and Clark et al. Therefore, it would have been obvious to a person of ordinary skill in the art the time the invention was made to include storing a encryption keys on a disk kept under physical surveillance with in the system of Colon et al. and Clark et al. with the motivation of preventing unauthorized access to valuable data thereby ensuring the privacy and security of the information.

As per claim 51, it is rejected for the same reasons set forth in claim 21.

7. Claims 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,731 to Colon et al. and U.S. Patent No. 6,171,112 to Clark et al. in view of U.S. Patent No. 6,272,470 to Teshima.

As per claims 22-23, Colon et al. and Clark et al. teach method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is

Art Unit: 3626

done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18).

Colon et al. and Clark et al. fail to explicitly teach shareware encryption protocol that is Pretty Good Privacy.

Teshima teaches an electronic clinical recording system that includes encrypting/decrypting software referred to as PGP (Pretty Good Privacy) using public keys (see: column 15, lines 34-41).

One of ordinary skill in the art at the time the invention was made would have found it obvious to include encrypting/decrypting software such as PGP (Pretty Good Privacy) with the system of Colon et al. and Clark et al. with the motivation of preventing unauthorized access to valuable data thereby ensuring the privacy and security of the information.

#### ***Response to Arguments***

8. Applicant's arguments filed 7/21/03 have been fully considered but they are not persuasive. Applicant's arguments will be addressed hereinbelow in the order in which they appear in the response filed 7/21/03.

(A) In the remarks, Applicants argue in substance that the Colon system cannot support an individual providing an electronic signature because individual are not authorized users of the Colon system and Clark does not teach individual providing an electronic signature for releasing personal or medical information.

In response to Applicant's argument that, the Examiner respectfully submits that the Clark et al. reference, and not Colon et al., *per se*, that was relied upon for the specific teaching of a method and apparatus for authenticating informed consent for patient that includes providing



Art Unit: 3626

a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50). Colon et al. was relied for primarily teaching of an Internet-networked system with online communication to a computing center from a large number of clinical study investigators at numerous and diverse locations remote from the computing center (see: column 1, lines 36-38). Thus, the proper combination of the applied references would the incorporation of Clark's authenticating informed consent for patient within Colon's method for managing data used in conducting clinical studies.

#### *Conclusion*

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Art Unit: 3626


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert W. Morgan whose telephone number is (703) 605-4441.

The examiner can normally be reached on 8:30 a.m. - 5:00 p.m. Mon - Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on (703) 305-9588. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

RWM  
rwm

  
JOSEPH THOMAS  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3600